UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

TASHAYIA BUSBY, DAMIEN ROSS, individually and on behalf of all those similarly situated, Plaintiffs, v. CAPITAL ONE FINANCIAL CORPORATION, CAPITAL ONE, N.A., CAPITAL ONE BANK (USA), N.A., AMAZON.COM, INC., and AMAZON WEB SERVICES, INC., Defendants.	NO. **CLASS ACTION COMPLAINT** **JURY DEMAND**

1. Plaintiff Tashayia Busby, and Damien Ross ("Plaintiffs"), on behalf of themselves, and all others similarly situated (the "Class"), bring this class action complaint against Defendants Amazon.com, Inc. ("Amazon") and Amazon Web Services, Inc. ("AWS") (collectively, the "Amazon Defendants") and Capital One Financial Corporation, Capital One, N.A., Capital One Bank (USA) (collectively, the "Capital One Defendants" or "Capital One"). Plaintiffs allege as follows upon personal knowledge as to their own acts and experience, and upon information and belief and the investigation of their attorneys as to all other matters:

INTRODUCTION

2. Plaintiffs bring this class action lawsuit on their behalf, and on behalf of the Class, against Capital One and the Amazon Defendants for their failure to protect the confidential information of over 100 million consumers including: names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, income, credit scores, credit limits, balances, payment history, contact information, transaction data, as well as approximately 140,000 social

security numbers and approximately 80,000 bank account numbers (collectively "PII").

3. On July 29, 2019, Capital One publicly announced that "there was unauthorized access by an outside individual who obtained certain types of personal information relating to people who had applied for its credit card products and to Capital One credit card customers." (the "Data Breach").

4. Through its failure to adequately protect Plaintiffs' and the Class members' PII, the Amazon Defendants and Capital One allowed Paige A. Thompson ("Thompson"), a former Amazon employee, to obtain access to and to surreptitiously view, remove, and make public Plaintiffs' and the Class members' PII entrusted to Capital One, as well as the Amazon Defendants.

5. At all relevant times, Capital One—through its Notice of Privacy Practices and other written assurances—promised to safeguard and protect Plaintiffs' and the Class members' PII in accordance with, federal, state and local laws, and industry standards. Capital One breached this promise.

6. Had Capital One informed Plaintiffs and Class members that Capital One would use inadequate security measures or entrust their PII to business associates that utilized inadequate security measures, Plaintiffs and the Class members would not have provided their PII to Capital One.

7. Capital One's and the Amazon Defendants' failures to implement adequate security protocols jeopardized the PII of millions of consumers, including Plaintiffs and the Class members, fell well short of Defendants' promises and obligations, and fell well short of Plaintiffs' and other Class members' reasonable expectations for protection of the PII they provided to Capital One who in turn provided such information to Amazon Defendants.

8. As a result of Capital One's and the Amazon Defendants' conduct and the ensuing Data Breach, Plaintiffs and the members of the proposed Class have suffered actual damages, failed to receive the benefit of their bargains, lost the value of their private data, and are at imminent risk of future harm, including identity theft and fraud which would result in further monetary loss. Accordingly, Plaintiffs bring suit, on behalf of themselves and the Class, to seek redress for Defendants' unlawful conduct.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000.00 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists.

10. This Court has personal jurisdiction over the Capital One Defendants because they are headquartered in and regularly conduct business in Virginia. In this District, the Capital One Defendants make decisions regarding corporate governance, management, security and information technology, including decisions regarding the security measures to protect the Personal Information that its stores. From this District, the Capital One Defendants negotiate and enter into agreements with businesses, such as the Amazon Defendants, to store Personal Information for those businesses on their servers and to provide other business services. The Capital One Defendants intentionally avail themselves of this Court's jurisdiction by conducting corporate operations here and promoting, selling and marketing its services from this District to millions of consumers worldwide.

11. This Court has personal jurisdiction over the Amazon Defendants because they are authorized to and regularly conduct business in Washington and have sufficient minimum

contacts in Washington such that the Amazon Defendants intentionally avail themselves of this Court's jurisdiction by conducting operations here, negotiating with the Capital One Defendants headquartered in this District, and promoting, selling and marketing its services to customers in this District.

12. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because the Amazon Defendants' headquarters and principal place of business are located in this District, and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this District, including, without limitation, decisions made by the Capital One Defendants' governance and management personnel or inaction by those individuals that led to misrepresentations, invasions of privacy and the Data Breach. Moreover, the Amazon Defendants maintain offices in this District, conducts business in this District, and entered into contractual relations with the Capital One Defendants headquartered in this District.

PARTIES

13. Plaintiff Tashayia Busby is a resident and a citizen of North Carolina. She has been a Capital One credit card holder since 2016. She received notice from Capital One that her PII was compromised in the Data Breach of Capital One's database, which was hosted by the Amazon Defendants. As a result of the Data Breach, Plaintiff Busby has had to carefully review her financial accounts to guard against fraud, failed to receive the benefit of her bargain, lost the value of her private data, and is at imminent risk of future harm, including identity theft and fraud which would result in further monetary loss. Additionally, Plaintiff Busby has discovered at least one instance of fraud on her Capital One card, which involved an individual charging her card for transportation services.

14. Plaintiff Damien Ross is a resident and citizen of Ohio. He currently has two

active Capital One credit cards that he applied for and obtained in 2019, prior to the Data Breach of Capital One's database. On information and belief, his PII was compromised in the Data Breach of Capital One's database, which was hosted by the Amazon Defendants. As a result of the Data Breach, Plaintiff Ross has had to carefully review his financial accounts to guard against fraud, failed to receive the benefit of his bargain, lost the value of his private data, and is at imminent risk of future harm, including identity theft and fraud which would result in further monetary loss. Additionally, Plaintiff Ross discovered fraudulent activity on his Capital One credit cards after the breach—with the latest occurrence of such fraud being in July 2019.

Amazon Defendants

15. Defendant Amazon.com, Inc. is a corporation existing under the laws of the State of Delaware with its headquarters and principal place of business located in the State of Washington at 410 Terry Ave. North, Seattle, WA 98109-5210.

16. Defendant Amazon Web Services, Inc. is a corporation existing under the laws of the State of Delaware with its headquarters and principal place of business located at 410 Terry Ave. North, Seattle, WA 98109-5210. Amazon Web Services, Inc. is a subsidiary of Amazon.com, Inc.

Capital One Defendants

17. Defendant Capital One Financial Corporation is a corporation existing under the laws of the State of Delaware with its headquarters and principal place of business located in the Commonwealth of Virginia at 1680 Capital One Drive, McLean, VA, 22102-3491.

18. Defendant Capital One, NA is a corporation with its principal place of business located at 1680 Capital One Drive, McLean, VA, 22102-3491. Capital One, NA is a wholly owned subsidiary of Capital One Financial Corporation.

19. Defendant Capital One Bank (U.S.A.), NA is a corporation with its principal place of business located at 1680 Capital One Drive, McLean, VA, 22102-3491. Capital One Bank (U.S.A.), NA is a wholly owned subsidiary of Capital One Financial Corporation.

FACTUAL BACKGROUND

Defendants' Collection and Storage of PII

20. Capital One is a bank holding company specializing in credit cards and offering other credit, including car loans and bank accounts. Capital One offers credit cards and other services to customers throughout the United States. Capital One solicits potential customers to provide them with sensitive PII through applications for credit cards and other financial products.

21. Capital One supports its consumer services, in part, by renting cloud-based storage provided by AWS, where it hosted credit card applications and materials containing customer PII.

22. Cloud computing has boomed as companies have increasingly turned to providers such as Amazon to do the work of configuring computers inside their own data centers. The processing power of those servers and storage devices is then rented out to cloud customers, who pay depending on how much work the computers do.

23. Capital One was an early adopter of cloud-computing among financial institutions, as many other banks hesitated to move sensitive customer data out of their data centers. Capital One started working with AWS in 2014 and has since become a marquee customer. In 2015, Capital One Chief Information Officer Rob Alexander said "the financial services industry attracts some of the worst cybercriminals. So we worked closely with the Amazon team to develop a security model, which we believe enables us to operate more securely in the public cloud than we can even in our own data centers."

24. According to published reports, the Capital One Defendants here stored Plaintiffs' and the Class' credit card applications containing PII in its cloud computer storage, which was provided by AWS.

25. The Amazon Defendants, through Defendant AWS, provide information technology infrastructure services to businesses like the Capital One Defendants in the form of various web services.[1] AWS offers a range of services, including Amazon Elastic Compute Cloud ("EC2") and Amazon Simple Storage Service ("Amazon S3" or "S3").[2]

26. According to AWS, Amazon S3 "is an object storage service that offers industry-leading scalability, data availability, security, and performance." S3 allows AWS customers to "*store and protect any amount of data*" for a range of use cases, including websites, mobile applications, backup and restore, archive, enterprise applications, Internet of Things ("IoT") devices, and big data analytics. AWS states that S3 provides easy-to-use management features so customers can organize data and configure finely-tuned access controls to meet their specific business, organizational, and compliance requirements.[3]

27. For S3 security, customers only have access to the S3 resources they create. A customer can grant access to other users by using one or a combination of the following access management features: AWS Identity and Access Management ("IAM") to create users and manage their respective access; Access Control Lists ("ACLs") to make individual objects accessible to authorized users; bucket policies to configure permissions for all objects within a

[1] *See* Amazon Web Services, https://craft.co/amazon-web-services (last accessed July 31, 2019).

[2] *See* Amazon EC2, https://aws.amazon.com/ec2/ (last accessed July 31, 2019) and Amazon Simple Storage Service, https://aws.amazon.com/s3/ (last accessed July 31, 2019).

[3] *See* Amazon Simple Storage Service, https://aws.amazon.com/s3/ (last accessed July 31, 2019) (emphasis added).

single S3 bucket; and Query String Authentication to grant time-limited access to others with temporary URLs.[4]

28. AWS notes that "[b]y default, all Amazon S3 resources—buckets, objects, and related subresources . . . are private: only the resource owner, an AWS account that created it, can access the resource."[5]

29. AWS also provides "Amazon GuardDuty" for customers to protect against unwanted threats. AWS declares that "Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads." GuardDuty works by using "machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats." In fact, AWS notes that GuardDuty helps "detect activity such as . . . credential compromise behavior, communication with known command-and-control servers, or API calls from known malicious IPs."[6]

Defendants' Professed Commitment to Data Security

30. AWS makes a public commitment to the security of data stored on its servers:

> At AWS, security is our highest priority. We design our systems with your security and privacy in mind.
>
> - We maintain a wide variety of compliance programs that validate our security controls. . . .
> - We protect the security of your information during transmission to or from AWS websites, applications, products, or services by using encryption protocols and software.
> - We follow the Payment Card Industry Data Security Standard (PCI DSS) when handling credit card data.

[4] *See* Amazon S3 Features, https://aws.amazon.com/s3/features/#Access_management_and_security (last accessed July 31, 2019).

[5] *See* Identity and Access Management, https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html (last accessed July 31, 2019).

[6] *See* Amazon GuardDuty, https://aws.amazon.com/guardduty/ (last accessed August 1, 2019).

- We maintain physical, electronic, and procedural safeguards in connection with the collection, storage, and disclosure of personal information. Our security procedures mean that we may request proof of identity before we disclose personal information to you.[7]

31. Similarly, the Capital One Defendants promise they are "committed to protecting your personal and financial information. If we collect identifying information from you, we will protect that information with controls based upon internationally recognized security standards, regulations, and industry-based best practices."[8]

32. Capital One's "Privacy Frequently Asked Questions" states:

> Capital One understands how important security and confidentiality are to our customers, so we use the following security techniques, which comply with or even exceed federal regulatory requirements to protect information about you:
>
> We maintain . . . electronic safeguards, such as passwords and encryption; and procedural safeguards, such as customer authentication procedures to protect against ID theft.
>
> We restrict access to information about you to authorized employees who only obtain that information for business purposes.
>
> We carefully select and monitor the outside companies we hire to perform services for us, such as mail vendors who send out our statements. We require them to keep customer information safe and secure, and we do not allow them to use or share the information for any purpose other than the job they are hired to do.[9]

33. The Frequently Asked Questions web page further states:

> We have taken the following steps to ensure secure Internet services:
>
> We protect our systems and networks with firewall systems.

---

[7] AWS Privacy Notice, Last Updated: December 10, 2018, https://aws.amazon.com/privacy/ (last accessed July 30, 2019).

[8] Capital One Online & Mobile Privacy Statement, https://www.capitalone.com/identity-protection/privacy/statement (last accessed July 30, 2019).

[9] *See* Privacy Frequently Asked Questions, https://www.capitalone.com/identity-protection/privacy/faq (emphasis added) (last accessed July 30, 2019).

> We employ Intrusion Detection software and monitor for unauthorized access.
>
> We maintain and selectively review activity logs to prevent unauthorized activities from occurring within our computing environment.
>
> We use encryption technology to protect certain sensitive information that is transmitted over the Internet.[10]

34. Further, Capital One's "Privacy and Opt Out Notice" stated: "To protect your personal information from unauthorized access and use, **we use security measures that comply with federal law**. These measures include computer safeguards and secured files . . . ."[11]

35. Similarly, Capital One's "Social Security Number Protections" disclosure stated:

> Capital One protects your Social Security Number. Our policies and procedures: 1) Protect the confidentiality of Social Security numbers; 2) Prohibit the unlawful disclosure of Social Security numbers; and 3) Limit access to Social Security numbers to employees or others with legitimate business purposes.
>
> These safeguards apply to all Social Security numbers collected through any channel or retained in any way by Capital One in connection with customer, employee or other relationships.[12]

36. Unfortunately for Plaintiffs and the Class, Defendants failed to live up to these explicit, as well as other implicit promises about the security of customer PII.

The Capital One Data Breach

37. On July 29, 2019, Capital One announced that the PII of more than 100 million individuals had been compromised.[13]

---

[10] *Id.* (emphasis added).

[11] *See* Capital One Privacy Notice, https://www.capitalone.com/privacy/notice/en-us/ (emphasis added) (last accessed July 31, 2019).

[12] *See* Social Security Number Protections, https://www.capitalone.com/identity-protection/privacy/social-security-number (emphasis added) (last accessed July 31, 2019).

[13] Press Release, Capital One (July 29, 2019), https://www.capitalone.com/facts2019/

38. According to Capital One, the Data Breach compromised "information on consumers and small businesses as of the time they applied for one of our credit card products from 2005 through early 2019," and included "names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, . . . self-reported income[,] . . . credit scores, credit limits, balances, payment history, contact information" and "transaction data."[14]

39. Capital One also disclosed that the Data Breach compromised the social security numbers of approximately 140,000 of the bank's credit card customers, and the bank account numbers of approximately 80,000 of the bank's secured credit card customers.[15]

40. The Data Breach was executed by Paige A. Thompson (a/k/a "erratic"), a former "systems engineer" for Amazon. On July 29, 2019, the FBI arrested, and federal prosecutors charged, Thompson in the United States District Court for the Western District of Washington with computer fraud and abuse in violation of 18 U.S.C. § 1030(a)(2).

41. Because Thompson is a former employee at Amazon's web services unit, the world's biggest cloud-computing business, that raises questions about whether she used knowledge acquired while working at the cloud-computing giant to commit her alleged crime, said Chris Vickery director of cyber-risk research at the security firm UpGuard Inc.

42. According to the criminal complaint, Thompson was able to gain access to PII collected by Capital One and stored on Capital One and AWS' systems. Thompson exploited a "configuration vulnerability" to gain access to the systems.[16] According to Capital One, this

---

[14] *Id.*

[15] *Id.*

[16] Frequently Asked Questions, Capital One (July 31, 2019), https://www.capitalone.com/facts2019/2/.

"unauthorized access also enabled the decrypting of data."[17]

43. Published reports suggest that the attacker exploited a type of vulnerability known as Server-Side Request Forgery (SSRF) to perform the attack.[18] By exploiting an SSRF vulnerability, an attacker can trick a server into disclosing sensitive server-side information that would otherwise be inaccessible outside the firewall.[19] In this case, reports suggest that Thompson was able to use SSRF to execute a request on an AWS EC2 instance controlled by Capital One that revealed Capital One's S3 credentials.[20]

44. This attack was possible due to a ***known*** vulnerability in AWS, that Amazon Defendants have failed to correct, that allows SSRF attackers to trick AWS EC2 instances into disclosing an AWS users' credentials.[21] The single-line command that exposes AWS credentials on any EC2 system is known by AWS and is in fact included in their online documentation.[22] It is also well known among hackers.

45. SSRF is a known vulnerability and Amazon Defendants have done nothing to fix it.

46. Thompson initially gained access to Capital One's systems on March 22, 2019, and the breach continued through at least April 21, 2019.[23]

---

[17] *Id.*

[18] *See* Early Lessons from the Capital One Data Breach, Stratum Security (July 31, 2019) https://blog.stratumsecurity.com/2019/07/31/early-lessons-from-the-capital-one-breach/ (last accessed August 1, 2019).

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] *See* IAM Roles for Amazon EC2, https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html (last accessed August 1, 2019).

[23] *Id.*

47. In a June 16, 2019 tweet, Thompson described a method for gaining access to files stored on AWS S3 systems that appears to closely match the method used to access Capital One's data:

48. Notably, the attack vector described by Thompson in her June 16, 2019 tweet **is not limited to Capital One's systems**. Rather, it exploits a general vulnerability of certain configurations of AWS S3 systems in general using a widely known vulnerability of which the Amazon Defendants were aware and could have prevented.

49. In fact, Thompson was apparently able to take advantage of this AWS configuration vulnerability to breach a number of other large corporations and organizations through the AWS network, including "one of the world's biggest telecom providers, an Ohio government body and a major U.S. university."[24]

[24] *See* Thomas Brewster, *DOJ Says Capital One Mega Breach Suspect Could Face More Charges—Did She Hack Multiple Companies?*, Forbes (July 30, 2019), https://www.forbes.com/sites/thomasbrewster/2019/07/30/capital-one-mega-breach-suspect-may-have-hacked-many-more-companies (last accessed July 31, 2019); *see also* Paige A. Thompson Criminal Complaint, Case No. MJ19-0344 ¶ 25 (W.D. Wash.) ("I understand this

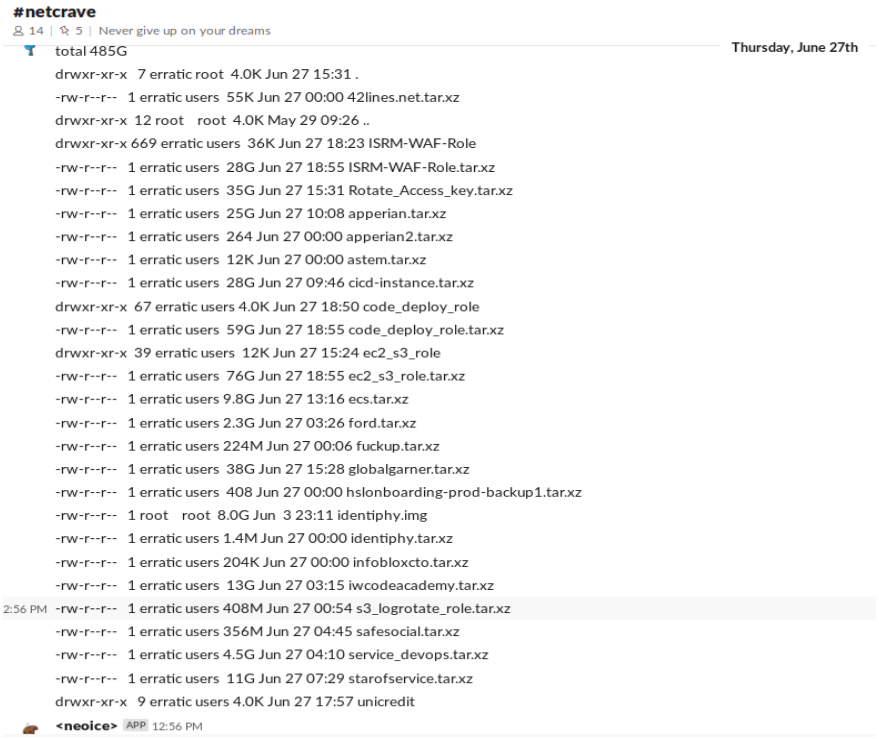
50. The FBI has confirmed that it is examining whether Thompson hit other targets like Michigan State, the Ohio Department of Transportation, UniCredit SpA (Italy's largest bank), and Ford. As the *Wall Street Journal* reported, "the widening probe points up a possible weakness: A hacker who figures out a way around the security fence of one cloud customer not only gets to that customer's data but also has a method that might be usable against others."[25]

51. Thompson further posted a comment in a public chatroom on the chat platform Slack on June 27, 2019, showing other chatroom participants hundreds of gigabytes of files she had apparently exfiltrated from various targets using the same AWS configuration vulnerability.[26] The following is a screenshot of Thompson's Slack comment, which includes names of a number of large companies and organizations:

post to indicate, among other things, that PAIGE A. THOMPSON intended to disseminate data from *victim entities, starting with Capital One*.") (emphasis added).

[25] Anuj Gangahar and Dana Mattioli, *FBI Examining Possible Data Breaches Related to Capital One*, Wall Street Journal (July 31, 2019), https://www.wsj.com/articles/italys-unicredit-investigating-data-breach-possibly-related-to-capital-one-11564587592 (last accessed July 31, 2019).

[26] *See* Brian Krebs, *Capital One Data Theft Impacts 106M People*, Krebs On Security, https://krebsonsecurity.com/2019/07/capital-one-data-theft-impacts-106m-people/ (last accessed July 31, 2019).



52. Despite these public boasts, Defendants did not discover the breach until four months after Thompson initially gained access to the breached data through the AWS configuration vulnerability, when an unknown third party emailed the Capital One Defendants on July 17, 2019.[27]

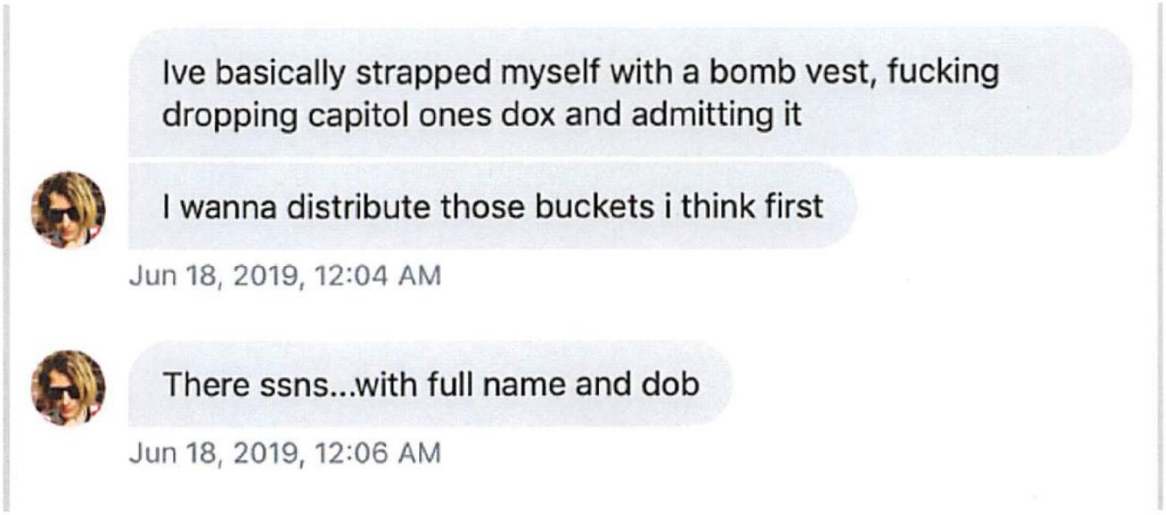
Dissemination of Breached Data

53. According to the criminal complaint, Thompson "intended to disseminate data stolen from victim entities, starting with Capital One."[28] As shown in the image below from the criminal complaint, Thompson stated that "I wanna distribute those buckets," and noted that the Capital One data included "ssns...with full name and dob."[29]

[27] https://www.capitalone.com/facts2019/

[28] Thompson Criminal Complaint, at 12.

[29] *Id.* at 11–12.



54. It appears that Thompson succeeded in disseminating the hacked information. According to the third party who notified Capital One of the Data Breach, some of the bank's internal data, which had been stored on the AWS S3 platform, had been posted publicly on the code-sharing and easily accessible website GitHub.[30]

55. The GitHub page referenced by the third party also included executable code, which Capital One confirmed "function[ed] to obtain Capital One's credentials, to list or enumerate folders or buckets of data, and to extract data from certain of those folder or

[30] *Id.* at 5–6.

buckets."[31]

56. It's not yet clear how many other hackers or individuals may have downloaded Capital One's data or exploited its credentials.

57. Capital One said it expected to spend up to $150 million to cover breach-related costs, largely for issues such as notifying customers and paying for credit monitoring. The bank has discussed potential fines or reimbursement to consumers.

Data Security Breaches Lead to Increased Actual and Potential Identity Theft.

58. Defendants knew or should have known that the PII that they were collecting from Plaintiffs and Class members, which was stolen during the Data Breach, was highly valuable and highly sought-after by criminals.

59. There has been an "upward trend in data breaches over the past 9 years, with 2018 seeing more data breaches reported than any other year since records first started being published."[32]

60. The United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report") that identity thieves use personally identifying data to open financial accounts, receive government benefits and incur charges and credit in a person's name.[33] As the GAO Report notes, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

---

[31] *Id*. at 7.

[32] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last accessed July 31, 2019).

[33] *See* United States Government Accountability Office, *Personal Information: Data Breaches Are Frequent, But Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), http://www.gao.gov/new.items/d07737.pdf.

61. In addition, the GAO Report makes clear that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[34]

62. Identity theft victims must often spend countless hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information such as social security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[35]

63. With access to an individual's PII, criminals can do more than just empty a victim's bank account; they can also commit many types of fraud, including: obtaining a driver's license or other official identification card in the victim's name but with the thief's picture on it; using the victim's name and social security number to obtain government benefits; and filing a fraudulent tax return using the victim's PII. In addition, identity thieves may obtain a job using the victim's PII, rent a house or receive medical services, prescription drugs and goods, and cause fraudulent medical bills to be issued in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued against the identity theft victim.[36] Further, loss of private and personal health information can expose the victim to loss of reputation, loss of employment, blackmail and other negative effects.

---

[34] *Id.*

[35] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

[36] *See Warning Signs of Identity Theft*, Federal Trade Commission, *available at* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed July 31, 2019).

64. PII is a valuable commodity to identity thieves. Compromised PII is traded on the "cyber black-market." As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, social security numbers, and other PII directly on various dark web[37] sites making the information publicly available.[38]

CLASS ALLEGATIONS

65. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class ("Class"):

> All persons in the United States whose PII was provided to the Capital One Defendants and maintained on the Amazon Defendants' servers and/or cloud computing systems that were compromised as a result of the data breach announced by Capital One on or around July 29, 2019.

66. Excluded from the Class are Defendants, their parents, subsidiaries, agents, officers and directors. Also excluded from the Class are any judicial officer assigned to this case and members of his or her staff.

67. Plaintiffs seek class certification pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3). In the alternative, Plaintiffs seeks class certification under Fed. R. Civ. P. 23(c)(4) because the common questions listed herein predominate as to particular issues that could substantially advance the litigation. The proposed Class meet the applicable requirements for certification under Fed. R. Civ. P. 23.

---

[37] The dark web refers to online content that cannot be found using conventional search engines and can be accessed only through specific browsers and software. MacKenzie Sigalos, *The Dark Web and How to Access It*, CNBC (Apr. 14, 2018), https://www.cnbc.com/2018/04/13/the-dark-web-and-how-to-access-it.html (last accessed July 31, 2019).

[38] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian Blog (Mar. 11, 2019), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed July 31, 2019); McFarland et al., *The Hidden Data Economy* 3, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf (last accessed July 31, 2019).

68. **Numerosity**: According to Defendants' public statements, the Data Breach affected approximately 106 million Capital One customers, making joinder of each individual member impracticable. Members of the Class are easily identifiable from Defendants' records.

69. **Commonality and Predominance**: Questions of law and fact common to the claims of Plaintiffs and the other members of the Class predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

- Whether Defendants failed to adequately safeguard Plaintiffs' and the Class members' PII;
- Whether Defendants failed to protect or otherwise keep Plaintiffs' and the Class members' PII secure, as promised;
- Whether Defendants' storage of Plaintiffs' and the Class members' PII violated federal, state, local laws, or industry standards;
- Whether Defendants engaged in unfair or deceptive practices by failing to properly safeguard Plaintiffs' and the Class members' PII, as promised;
- Whether Defendants violated the consumer protection statutes applicable to Plaintiffs and the members of the Class;
- Whether Defendants failed to notify Plaintiffs and members of the Class about the Data Breach as soon as practical and without delay after the Data Breach was discovered;
- Whether Defendants acted negligently in failing to safeguard Plaintiffs' and the Class members' PII; and
- Whether Plaintiffs and the members of the Class are entitled to damages as a result of Defendants' conduct.

70. **Typicality**: Plaintiffs' claims are typical of the claims of the members of the Class. Plaintiffs and the members of the Class sustained damages as a result of Defendants' uniform wrongful conduct during transactions with them, including their storage and transmission of the PII and failure to adequately safeguard it.

71. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests

of the Class and has retained counsel competent and experienced in complex litigation and class actions. Plaintiffs have no interests antagonistic to those of the Class, and Defendants have no defenses unique to Plaintiffs. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Class.

72. **Risks of Prosecuting Separate Actions**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications, which would establish incompatible standards of conduct for the Defendants or would be dispositive of the interests of members of the proposed Class.

73. **Policies Generally Applicable to the Class**: This class action is appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Plaintiffs and proposed Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendants' lax data security protocols and practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiffs' challenges to those practices hinge on Defendants' conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiffs.

74. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual

prosecution of the litigation necessitated by Defendants' conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendants. Even if members of the Class could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

CAUSES OF ACTION

Count I
Negligence
(Against All Defendants on Behalf of Plaintiffs and the Class)

75. Plaintiffs re-allege and incorporates by reference all preceding allegations as if set forth in this Count.

76. The Capital One Defendants required Plaintiffs and the Class members to submit sensitive personal information, including PII and non-public personal and financial information, in order to obtain services.

77. The Capital One Defendants stored this PII on the Amazon Defendants' cloud-computing platforms.

78. By collecting and storing this data, Defendants had a duty of care to use reasonable means to secure and safeguard this PII, to prevent disclosure of the information, and to guard the information from theft.

79. Defendants assumed a duty of care to use reasonable means and implement policies and procedures to prevent unauthorized access to this PII.

80. Defendants had a duty to monitor, supervise, or otherwise provide oversight to safeguard the PII they collected and stored on the Amazon Defendants' cloud computing platforms.

81. Furthermore, given the other major data breaches affecting the healthcare and financial industries, Plaintiffs and the Class are part of a well-defined, foreseeable, finite, and discernible group that was at high risk of having their PII stolen.

82. Defendants owed a duty to Plaintiffs and members of the Class to provide security consistent with industry standards, statutory requirements, and the other requirements discussed herein, and to ensure that their systems and networks—and the personnel responsible for them—adequately protected their patients' or customers' PII.

83. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants, on the one hand, and Plaintiffs or the other Class members, on the other hand. The special relationship arose because Plaintiffs and the members of the Class entrusted Defendants with their PII as part of their applications for credit cards with the Capital One Defendants. Defendants alone could have ensured that their systems were sufficient to prevent or minimize the Data Breach.

84. In addition, Defendants had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair. . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data by entities like Defendants.

85. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the common law and the statutes and regulations described above, but also

because it was bound by, and had committed to comply with, industry standards for the protection of confidential PII.

86. Defendants knew or should have known that the Amazon Defendants' cloud computing systems were vulnerable to unauthorized access.

87. Defendants breached their common law, statutory and other duties—and thus, were negligent—by failing to use reasonable measures to protect consumers' PII from hackers, failing to limit the severity of the Data Breach, and failing to detect the Data Breach in a timely fashion.

88. It was foreseeable that Defendants' failure to use reasonable measures to protect consumers' PII from attackers, failure to limit the severity of the Data Breach, and failure to detect the Data Breach in a timely fashion, would result in injury to Plaintiffs and the members of the Class. Further, the breach of security, unauthorized access, and resulting injuries to Plaintiffs and the Class were reasonably foreseeable, particularly in light of the other major data breaches affecting the healthcare and financial industries.

89. It was therefore reasonably foreseeable that Defendants' breaches of duties and failure to adequately safeguard PII would, and in fact did, result in one or more of the following injuries to Plaintiffs and the Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings;

lost work time; lost value of the PII; lost benefits of their bargains; and other economic and non-economic harm.

90. Accordingly, Plaintiffs, on behalf of themselves and the members of the Class, seek an order declaring that Defendants' conduct constitutes negligence, and awarding damages in an amount to be determined at trial.

Count II
Negligence *Per Se*
(Against All Defendants on Behalf of Plaintiffs and the Class)

91. Plaintiffs re-allege and incorporate by reference all preceding allegations as if set forth in this Count.

92. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act"), prohibits "unfair . . . practices in or affecting commerce," including the unfair practices committed by Defendants in failing to use reasonable measures to protect Plaintiff and the Class' PII.

93. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to secure and protect PII, in defiance of industry standards. This violation constituted negligence per se.

94. Plaintiffs and the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

95. The harm that occurred as a result of the Data Breach is the type of harm that the FTC Act was designed to protect against. The FTC regularly pursues enforcement actions against businesses, such as Defendants, who fail to employ reasonable data security measures and, as a result, cause harm to consumers in the form of breached PII.

96. As a result of Defendants' negligence per se, Plaintiffs and the Class have been

injured and have sustained damages as alleged herein.

97. It was therefore reasonably foreseeable that Defendants' breaches of duties and failure to adequately safeguard PII would, and in fact did, result in one or more of the following injuries to Plaintiffs and the Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefits of their bargains; and other economic and non-economic harm.

98. Accordingly, Plaintiffs, on behalf of themselves and the members of the Class, seek an order declaring that Defendants' conduct constitutes negligence per se, and awarding damages in an amount to be determined at trial.

Count III
Breach of Contract
(Against Capital One Defendants on Behalf of Plaintiffs and the Class)

99. Plaintiffs re-allege and incorporate by reference all preceding allegations as if set forth in this Count.

100. When Plaintiffs and the Class provided their PII to Capital One in exchange for its services, they entered into contracts pursuant to which Capital One agreed to reasonably protect class members' PII.

101. Capital One solicited and invited class members to provide their PII as part of

Capital One's regular business practices. Plaintiffs and the Class accepted Capital One's offer and provided their PII to Capital One in connection with credit card applications.

102. In entering into such contracts, Plaintiffs and the Class reasonably believed and expected that Capital One's data security practices complied with relevant laws and regulations, were consistent with industry standards, and were consistent with the representations made in Capital One's privacy policy.

103. Class members who paid money to Capital One reasonably believed and expected that Capital One would use a portion of that money to implement adequate data security. Capital One failed to do so.

104. Plaintiffs and the Class would not have entrusted their PII to Capital One in the absence of the implied contract between them and Capital One to keep the PII reasonably secure.

105. Plaintiffs and the Class fully performed their obligations under the contracts with Capital One.

106. Capital One breached its contracts with class members by failing to safeguard and protect the PII.

107. As a direct and proximate result of Capital One's breaches of the contracts, Plaintiffs and the Class sustained damages as alleged herein.

108. Plaintiffs and the Class are entitled to recover compensatory and consequential damages suffered as a result of the Data Breach.

109. Plaintiffs and the Class are also entitled to injunctive relief requiring Capital One to, without limitation: (i) strengthen its data security systems; (ii) submit to future annual audits of its systems and monitoring procedures; and (iii) provide free credit monitoring and identity theft insurance for several years to all class members.

Count IV
Violation of the Washington Consumer Protection Act
(Against All Defendants on Behalf of Plaintiffs and the Class)

110. Plaintiffs re-allege and incorporate by reference all preceding allegations as if set forth in this Count.

111. Washington's Consumer Protection Act, RCW §§ 19.86.010, *et seq.* ("CPA"), promotes fair competition in commercial markets for goods and services for the protection of consumers.

112. The CPA prohibits any person from "using unfair methods of competition or unfair or deceptive acts or practices in the conduct of any trade or commerce . . . ." RCW § 19.86.020.

113. The Capital One and Amazon Defendants did not disclose that they failed to take reasonable steps to protect the security of PII collected and stored by them, PII that was ultimately compromised in the Data Breach.

114. Defendants' omissions had the capacity to deceive a substantial portion of the public.

115. Defendants accepted responsibility for the security of PII collected from Plaintiffs and members of the Class and stored on Capital One's AWS servers. Defendants were responsible for designing and implementing security procedures and protocols to ensure the security of that PII, and Defendants knew or should have known that they were not adequately protecting that data.

116. Defendants' conduct was a deceptive act or practice because it concealed their true lack of security in protecting this data.

117. Had Plaintiffs and the Class known that AWS servers storing their PII were

vulnerable to intrusion, such that an attacker was able to easily access and disseminate their PII, they would not have been willing to provide their PII to the Defendants.

118. Defendants' conduct in failing to provide reasonable data security protection for the Class' PII was an unfair act or practice.

119. As a result of Defendants' conduct, Plaintiffs and the Class sustained damages as alleged herein.

Count V
Violation of the Washington Data Breach Disclosure Law
(Against Defendants on Behalf of Plaintiffs and the Class)

120. Plaintiffs re-allege and incorporate by reference all preceding allegations as if set forth in this Count.

121. RCW § 19.255.010(2) provides that "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." *See* RCW § 19.255.010(2).

122. The Data Breach alleged herein resulted in "unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained by" Defendants and, therefore, experienced a "breach of the security of [their] system[s]," as defined by RCW § 19.255.010(4).

123. Defendants failed to disclose that the PII of over 100 million customers had been compromised immediately upon discovery of the Data Breach, and in doing so unreasonably delayed informing Plaintiffs and the Class about the Data Breach at the time they knew or should have known that the Data Breach had occurred. This failure is a violation of § 19.255.010.

PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and the Class, respectfully request that this Court enter an Order:

1. Certifying this case as a class action on behalf of Plaintiffs and the Class defined above, appointing Plaintiffs as Class Representatives of the Class, and appointing Plaintiffs' counsel to represent the Class;
2. Awarding Plaintiffs and the Class appropriate relief, including actual and statutory damages;
3. Awarding equitable, injunctive, and declaratory relief as may be appropriate, including without limitation an injunction and declaring Defendants' conduct to be unlawful;
4. Awarding Plaintiffs and the Class their reasonable litigation expenses and attorneys' fees;
5. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable by law;
6. Permitting Plaintiffs and the Class to amend their pleadings to conform to the evidence produced at trial; and
7. Awarding such other and further relief as equity and justice may require.

JURY DEMAND

Plaintiffs request a trial by jury.

DATED: August 13, 2019

Respectfully submitted,

By: *s/ Steven J. Toll*
Steven J. Toll

Steven J. Toll, VA Bar #15300
Andrew N. Friedman*

Douglas J. McNamara*
Karina Puttieva*
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue, NW, Suite 500
Washington, D.C. 20005
Tel.: 202.408.4600
stoll@cohenmilstein.com
afriedman@cohenmilstein.com
dmcnamara@cohenmilstein.com
kputtieva@cohenmilstein.com

TOUSLEY BRAIN STEPHENS PLLC
Kim D. Stephens*
Jason T. Dennett*
Kaleigh N.B. Powell*
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101
Tel.: 206.682.5600/Fax.: 206.682-2992
Email: kstephens@tousley.com
jdennett@tousley.com
kpowell@tousley.com

James J. Pizzirusso*
Swathi Bojedla*
Theodore F. DiSalvo*
HAUSFELD LLP
1700 K Street NW, Suite 650
Washington, D.C. 20006
Tel.: 202.540.7200
jpizzirusso@hausfeld.com
sbojedla@hausfeld.com
tdisalvo@hausfeld.com

Adam J. Levitt*
Amy E. Keller*
DICELLO LEVITT GUTZLER LLC
Ten North Dearborn Street
Eleventh Floor
Chicago, Illinois 60602
Tel.: 312.214.7900
alevitt@dicellolevit.com
akeller@dicellolevitt.com

E. Michelle Drake*
BERGER MONTAGUE, PC
43 SE Main Street, Suite 505
Minneapolis, MN 55414
Tel.: 612.594.5933
emdrake@bm.net

Daniel L. Warshaw*
Matthew A. Pearson*
PEARSON, SIMON & WARSHAW, LLP
15165 Ventura Boulevard, Suite 400
Sherman Oaks, California 91403
Tel.: 818.788.8300
dwarshaw@pswlaw.com
mapearson@pswlaw.com

Counsel for Plaintiffs and the Class

**Pro Hac Vice Applications to be Submitted*